

AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A public key generation apparatus including:

a random number generator for generating a random number k_a that holds a relationship $0 < k_a < q$, where an element in a finite group F for which multiplication is defined is g , and an order that is a prime number of the element g is q ; and

a public key generator for calculating a public key y_a in the finite group F from the random number k_a , the element g , and the prime number q ,

wherein at least said random number generator and said public key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the public key generator,

wherein the random number generator generates a new random number after the calculation of the public key y_a is completed so that the public key y_a becomes a function of the random number,

wherein a controller of a first user as a distribution source of the public key controls the random number generator and the public key generator to obtain the public key y_a , and transmits the obtained public key y_a to a second user as a distribution destination of the public key, and

wherein the arithmetic algorithm of the public key generator is not revealed outside of the one semiconductor integrated circuit.

2. (Previously Presented) The public key generation apparatus of Claim 1, wherein said public key generator calculates the public key y_a in the finite group F by a formula:

$ya = g^{ka} \bmod q$, using the random number ka , the element g , and the prime number q .

3. (Previously Presented) The public key generation apparatus of Claim 1, wherein when the finite group F is an elliptic curve $E(F)$ in a finite field, and an element of the elliptic curve $E(F)$ is G ,

said public key generator calculates the public key ya on the elliptic curve $E(F)$ by a formula: $ya = kaG \bmod q$, using the random number ka , the element G , and the prime number q .

4. (Canceled)

5. (Previously Presented) A shared key generation apparatus including:
a random number generator for generating a random number ka that holds a relationship $0 < ka < q$, where an element in a finite group F for which multiplication is defined is g , and an order that is a prime number of the element g is q ; and
a shared key generator for calculating a shared key Ka in the finite group F from a public key yb that is generated from a random number kb which holds a relationship $0 < kb < q$ and is generated by a second user as a distribution destination of the shared key, and the random number ka ,

wherein at least said random number generator and said shared key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the shared key generator,

wherein the random number generator generates a new random number after the calculation of the public key y_a is completed so that the shared key K_a becomes a function of the random number,

wherein a controller of a first user as a distribution source of the shared key obtains the public key y_b from the second user as the shared key distribution destination, and controls the random number generator and the shared key generator to derive the shared key K_a , and

wherein the arithmetic algorithm of the shared key generator is not revealed outside of the one semiconductor integrated circuit.

6. (Previously Presented) The shared key generation apparatus of Claim 5, wherein said shared key generator calculates the shared key K_a in the finite group F by a formula: $K_a = y_b^{k_a} \bmod q$, using the public key $y_b = g^{k_b} \bmod q$ which is generated by the second user as the shared key distribution destination and the random number k_a .

7. (Previously Presented) The shared key generation apparatus of Claim 5, wherein when the finite group F is an elliptic curve $E(F)$ in a finite field and an element of the elliptic curve $E(F)$ is G ,

said shared key generator calculates the shared key K_a on the elliptic curve $E(F)$ by a formula: $K_a = k_a y_b \bmod q$, using the public key $y_b = k_b G \bmod q$ which is generated on the elliptic curve $E(F)$ from the random number k_b by the second user as the shared key distribution destination, and the random number k_a .

8. (Canceled)

9. (Previously Presented) A key exchange apparatus including:

a random number generator for generating a random number k_a that holds a relationship $0 < k_a < q$, where an element in a finite group F for which multiplication is defined is g , and an order that is a prime number of the element g is q ;

a public key generator for calculating a public key y_a in the finite group F from the random number k_a , the element g , and the prime number q ; and

a shared key generator for calculating a shared key K_a in the finite group F on the basis of the public key y_b generated from a random number k_b which holds a relationship $0 < k_b < q$ and is generated by a second user as a distribution destination of the shared key, and the random number k_a ,

wherein at least said random number generator, said public key generator, and said shared key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of arithmetic algorithms of the public key generator and the shared key generator,

wherein the random number generator generates a new random number after the calculation of the public key y_a and the calculation of the shared key K_a are both completed so that the public key y_a and the shared key K_a become functions of the random number,

wherein a controller of a first user as a distribution source of the shared key controls the random number generator and the public key generator to obtain the public key y_b , and controls the shared key generation unit to derive the shared key K_a , and

wherein the arithmetic algorithms of the public key generator and the shared key generator are not revealed outside of the one semiconductor integrated circuit.

10. (Previously Presented) The key exchange apparatus of Claim 9, wherein said public key generator calculates the public key y_a in the finite group F by a formula: $y_a = g^{k_a} \text{ mod } q$, using the random number k_a , the element g , and the prime number q , and said shared key generator calculates the shared key K_a in the finite group F by a formula: $K_a = y_b^{k_a} \text{ mod } q$, using the public key $y_b = g^{k_b} \text{ mod } q$ which is generated in the finite group F by the second user as the shared key distribution destination using the random number k_b , and the random number k_a .

11. (Previously Presented) The key exchange apparatus of Claim 9, wherein when the finite group F is an elliptic curve $E(F)$ in a finite field, and an element of the elliptic curve $E(F)$ is G ,
said public key generator calculates the public key y_a on the elliptic curve $E(F)$ by a formula: $y_a = k_a G \text{ mod } q$, using the random number k_a , the element G , and the prime number q , and
said shared key generator calculates the shared key K_a on the elliptic curve $E(F)$ by a formula: $K_a = k_a y_b \text{ mod } q$, using the public key $y_b = k_b G \text{ mod } q$ generated from the random number k_b on the elliptic curve $E(F)$ by the second user as the shared key distribution destination, and the random number k_a .

12. (Cancelled)

13. (Previously Presented) A key exchange apparatus including:

a random number generator for generating a random number ka that holds a relationship $0 < ka < q$, where an element in a finite group F for which multiplication is defined is g , and an order that is a prime number of the element g is q ;

a secret key holding unit for temporarily holding the random number ka ;

a public key generator for calculating a public key ya in the finite group F from the random number ka , the element g , and the prime number q ; and

a shared key generator for calculating a shared key Ka in the finite group F using a public key yb generated from a random number kb which holds a relationship $0 < kb < q$ and is generated by a second user as a destination distribution of the shared key, and the random number ka that is held by the secret key holding unit,

wherein at least said random number generator, said secret key holding unit, said public key generator, and the shared key generator are formed on one semiconductor integrated circuit so as to prevent diversion or alteration of arithmetic algorithms of the public key generator and the shared key generator,

wherein the random number generator generates a new random number after the calculation of the shared key Ka is completed so that the public key ya and the shared key Ka become functions of the random number,

wherein said secret key holding unit holds the new random number generated by the random number generator,

wherein a controller of a first user as a distribution source of the shared key controls the random number generator and the public key generator to obtain the public key y_a , and transmits the obtained public key y_a to a second user as a distribution destination of the shared key,

wherein said controller obtains the public key y_b from the second user as the shared key distribution destination, and controls the shared key generator to derive the shared key K_a , and wherein the arithmetic algorithms of the public key generator and the shared key generator are not revealed outside of the one semiconductor integrated circuit.

14. (Previously Presented) The key exchange apparatus of Claim 13, wherein the public key generator calculates the public key y_a in the finite group F using the random number k_a , the element g , and the prime number q by a formula: $y_a = g^{k_a} \bmod q$, and the shared key generator calculates the shared key K_a in the finite group F by a formula: $K_a = y_b^{k_a} \bmod q$, using the public key $y_b = g^{k_b} \bmod q$ that is generated in the finite group F from the random number k_b by the second user as the shared key distribution destination, and the random number k_a that is held in the secret key holding unit.

15. (Previously Presented) The key exchange apparatus of Claim 13, wherein when the finite group F is an elliptic curve $E(F)$ in a finite field, and an element on the elliptic curve $E(F)$ is G , the public key generator calculates the public key y_a on the elliptic curve $E(F)$ using the random number k_a , the element G , and the prime number q by a formula: $y_a = k_a G \bmod q$, and

the shared key generator calculates the shared key K_a on the elliptic curve $E(F)$ by a formula: $K_a = K_a y_b \bmod q$, using the public key $y_b = k_b G \bmod q$ that is generated from the random number k_b on the elliptic curve $E(F)$ by the second user as the shared key distribution destination, and the random number k_a that is held in the secret key holding unit.

16. (Previously Presented) The key exchange apparatus of Claim 13, wherein the random number generator generates a new random number k_a after the calculation of the public key y_a is completed, and the secret key holding unit holds the new random number k_a generated by the random number generator.

17. (Cancelled)

18. (Previously Presented) A key exchanging method that employs the key exchange apparatus of Claim 9, thereby exchanging the public keys that are generated by a first user and a second user that intend to exchange the public keys, respectively, to generate a shared key by the first user and the second user on the basis of the exchanged public key, respectively.

19. (Previously Presented) A key exchanging method that employs the key exchange apparatus of Claim 13, thereby exchanging the public keys that are generated by a first user and a second user that intend to exchange the public keys, respectively, to generate a shared key by the first user and the second user on the basis of the exchanged public key, respectively.

20. (Currently Amended) The public key generation apparatus of claim 1, wherein the public key generator uses the random number key-ka in the one semiconductor integrated circuit only for the calculation of the public key ya.

21. (Currently Amended) The sharked key generation apparatus of claim 5, wherein the shared key generator uses the random number key-ka in the one semiconductor integrated circuit only for the calculation of the shared key Ka.

22. (Currently Amended) The key exchange apparatus of claim 9, wherein the shared key generator uses the random number key-ka in the one semiconductor integrated circuit only for the calculation of the public key ya and the shared key Ka.

23. (Currently Amended) The key exchange apparatus of claim 13, wherein the shared key generator uses the random number key-ka in the one semiconductor integrated circuit only for the calculation of the public key ya and the shared key Ka.